证书
SANtricity 11.5

NetApp
February 12, 2024

目录

证书

概念

CA证书的工作原理

证书颁发机构(Certificate Authority、CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。

打开浏览器并尝试通过控制器管理端口连接到System Manager时、浏览器会尝试验证存储阵列的控制器是否为可信源。如果浏览器找不到控制器的数字证书、则会向您发出警报、指出该证书未由可识别的颁发机构签名、并询问您是否要继续。如果您不想再看到此警报、则必须从CA获取签名的数字证书。

如果您使用的外部密钥管理服务器具有驱动器安全功能、则还可以创建用于在该服务器和控制器之间进行身份验证的证书、或者接受存储阵列中的自签名证书。

要使用可信颁发机构提供的数字证书、需要执行以下步骤：

1. 转到菜单：设置[证书]。您的用户登录名必须包含安全管理员权限；否则、*证书*不会显示在页面上。
2. 为每个控制器或密钥管理服务器创建证书签名请求(CSR)。
3. 将.csr文件发送到CA、然后等待这些文件向您发送证书。
4. 从CA导入可信(中间和根)证书。这些证书可为CA层次结构建立信任点。
5. 导入每个控制器或密钥管理服务器的已签名管理证书。

证书术语

了解证书条款如何应用于存储阵列。

期限	Description
CA	证书颁发机构(Certificate Authority、CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。
CSR	证书签名请求(CSR)是从申请人发送给证书颁发机构(CA)的一条消息。CSR会验证CA对证书进行问题描述 所需的信息。
证书	出于安全考虑、证书用于标识站点所有者、从而防止攻击者模拟站点。此证书包含有关站点所有者的信息以及对此信息进行认证(签名)的可信实体的身份。

期限	Description
客户端证书	对于安全密钥管理、客户端证书会验证存储阵列的控制器、以便密钥管理服务器可以信任其IP地址。
密钥管理服务器证书	对于安全密钥管理、密钥管理服务器证书会对服务器进行验证、以便存储阵列可以信任其IP地址。
管理证书	管理证书由证书颁发机构(CA)批准、并允许安全访问Web应用程序。也称为"签名证书"。
OCSP服务器	联机证书状态协议(OCSP)服务器可确定证书颁发机构(CA)是否已在计划的到期日期之前撤销任何证书、然后在证书被撤销时阻止用户访问服务器。
自签名证书	自签名证书会预先加载到控制器上。如果站点连接是自签名的、则会打开一条警告消息、然后您才能继续使用Web应用程序。
可信证书	证书颁发机构(CA)的可信证书是证书层次结构顶部的已知证书。也称为"根证书"。

操作说明

完成控制器的**CA**证书签名请求**(CSR)**

要接收存储阵列控制器的证书颁发机构(CA)证书、您必须先为存储阵列中的每个控制器生成证书签名请求(CSR)文件。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

关于此任务

此任务介绍如何生成要发送给CA以接收控制器的已签名管理证书的.csr文件(证书签名请求)。您必须提供有关您的组织的信息以及控制器的IP地址或DNS名称。在此任务期间、如果存储阵列中只有一个控制器、则会生成一个.csr文件；如果有两个控制器、则会生成两个.csr文件。

步骤

1. 选择菜单：设置[证书]。
2. 从*阵列管理*选项卡中、选择*完成CSR*。

> 如果显示一个对话框、提示您接受第二个控制器的自签名证书、请单击*接受自签名证书*以继续。

3. 输入以下信息、然后单击*下一步*：

- 组织—贵公司或组织的法定全名。包括后缀、例如Inc.或Corp.
- 组织单位(可选)—组织中负责处理证书的部门。
- 城市/位置—存储阵列或业务所在的城市。
- 省/自治区/直辖市(可选)—存储阵列或业务所在的省/自治区/直辖市。
- 国家/地区**ISO**代码—您所在国家/地区的两位数ISO (国际标准化组织)代码、例如美国。

> 某些字段可能会预先填充相应的信息、例如控制器的IP地址。请勿更改预先填充的值、除非您确定这些值不正确。例如、如果尚未完成CSR、则控制器IP地址将设置为"`localhost.`"。在这种情况下、您必须将"`localhost`"更改为控制器的DNS名称或IP地址。

4. 验证或输入有关存储阵列中控制器A的以下信息：
   - 控制器**A**公用名-默认情况下、显示控制器A的IP地址或DNS名称。请确保此地址正确无误；它必须与您在浏览器中输入的内容完全匹配、才能访问System Manager。
   - 控制器**A**备用**IP**地址-如果公用名称为IP地址、则可以选择为控制器A输入任何其他IP地址或别名对于多个条目、请使用逗号分隔格式。
   - 控制器**A**备用**DNS**名称-如果公用名是DNS名称、请为控制器A输入任何其他DNS名称对于多个条目、请使用逗号分隔格式。如果没有备用DNS名称、但您在第一个字段中输入了DNS名称、请将此名称复制到此处。如果存储阵列只有一个控制器、则可以使用*完成*按钮。如果存储阵列有两个控制器、则可以使用*下一步*按钮。

   > 首次创建CSR请求时、请勿单击*跳过此步骤*链接。在错误恢复情况下提供此链接。在极少数情况下、一个控制器上的CSR请求可能会失败、而另一个控制器上的CSR请求则可能不会失败。通过此链接、您可以跳过在已定义的控制器A上创建CSR请求的步骤、并继续执行在控制器B上重新创建CSR请求的下一步

5. 如果只有一个控制器、请单击*完成*。如果有两个控制器、请单击*下一步*以输入控制器B的信息(与上述相同)、然后单击*完成*。

   对于单个控制器、会将一个.csr文件下载到本地系统。对于双控制器、将下载两个.csr文件。下载内容的文件夹位置取决于您的浏览器。

6. 将.csr文件发送到CA。

完成后

收到数字证书后、请导入CA发送给您的相应证书文件。

导入控制器的可信证书

从证书颁发机构(CA)接收数字证书后、您可以导入控制器的证书链(中间和根)。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 您已生成证书签名请求(.csr文件)并将其发送到CA。
- CA返回了可信证书文件。
- 证书文件安装在本地系统上。

关于此任务

此任务介绍如何为存储阵列的控制器上传可信证书。

步骤

1. 选择菜单：设置[证书]。
2. 从*可信*选项卡中、选择*导入*。

   此时将打开一个对话框、用于导入可信证书文件。

3. 单击*浏览*以选择控制器的证书文件。

   文件名显示在对话框中。

4. 单击 * 导入 * 。

结果

这些文件将上传并进行验证。

完成后

导入管理证书。

导入控制器的管理证书

导入可信证书链后、您可以为存储阵列中的每个控制器导入一个管理(签名)证书文件。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 已导入可信证书。
- CA为每个控制器返回一个管理证书文件。
- 您的本地系统上提供了管理证书文件。

关于此任务

此任务介绍如何上传用于控制器身份验证的管理证书文件。

步骤

1. 选择菜单：设置[证书]。
2. 从*阵列管理*选项卡中、选择*导入*。

   此时将打开一个对话框、用于导入证书文件。

3. 单击*浏览*以选择控制器A的文件如果有两个控制器、请单击第二个*浏览*按钮为控制器B选择文件

   文件名将显示在对话框中。

4. 单击 * 导入 * 。

   文件已上传并进行验证。

结果

会话将自动终止。要使证书生效、您必须重新登录。重新登录后、新的CA签名证书将用于会话。

查看导入的证书信息

在证书页面中、您可以查看先前导入的证书的证书类型、颁发机构和有效日期范围。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

关于此任务

此任务介绍如何查看用户安装或预安装的证书的信息。

步骤

1. 选择菜单：设置[证书]。
2. 选择其中一个选项卡可查看有关控制器的管理证书、可信证书和密钥管理服务器的证书的信息。

选项卡	Description
阵列管理	查看有关为控制器导入的所有服务器证书的信息。
值得信赖	查看有关为控制器导入的所有受信任(根)证书的信息。使用*显示证书…*下的筛选器字段可查看用户安装或预安装的证书。 • 用户安装。用户上传到存储阵列的证书(包括可信证书、LDAPS证书和身份联合证书)。 • 预安装。存储阵列附带的证书。
密钥管理	查看有关为外部密钥管理服务器导入的所有管理(签名)证书的信息。

删除可信证书

您可以删除用户导入的任何证书。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 如果要使用新版本更新受信任证书、则必须先导入更新后的证书、然后才能删除旧证书。

如果在导入替代证书之前删除用于对存储阵列的管理证书或LDAP服务器进行身份验证的证书、则可能无法访问系统。

关于此任务

此任务介绍如何删除用户导入的证书。无法删除预定义证书。

步骤

1. 选择菜单：设置[证书]。
2. 选择*可信*选项卡。

   此表显示了存储阵列的受信任证书。

3. 从表中、选择要删除的证书。
4. 单击菜单：uncommon Tasks[Delete]。

   此时将打开确认删除可信证书对话框。

5. 在字段中键入`delete`、然后单击*删除*。

重置管理证书

您可以将存储阵列上的管理证书还原为出厂自签名状态。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 必须事先导入证书。

关于此任务

重置存储阵列上的管理证书会从每个控制器中删除当前的管理证书。重置证书后、控制器将还原为使用自签名证书。

步骤

1. 选择菜单：设置[证书]。
2. 从*阵列管理*选项卡中、选择*重置*。

   此时将打开一个*确认重置管理证书*对话框。

3. 在字段中键入`reset`、然后单击*重置*。

结果

浏览器刷新后、控制器将还原为使用自签名证书。因此、系统会提示用户为其会话手动接受自签名证书。

完成密钥服务器的**CA**证书签名请求**(CSR)**

要接收密钥管理服务器的证书颁发机构(CA)证书、必须先生成证书签名请求(CSR)文件。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

关于此任务

此任务介绍如何生成要发送给CA以接收密钥管理服务器的签名证书的.csr文件(证书签名请求)。在此任务期间、您必须提供有关您的组织的信息。

步骤

1. 选择菜单：设置[证书]。
2. 从*密钥管理*选项卡中、选择*完成CSR*。
3. 输入以下信息：
   - 公用名—用于标识此CSR的名称、例如存储阵列名称、该名称将显示在证书文件中。
   - 组织—贵公司或组织的法定全名。包括后缀、例如Inc.或Corp.
   - 组织单位(可选)—组织中负责处理证书的部门。
   - 城市/位置-组织所在的城市或位置。
   - 省/自治区/直辖市(可选)—组织所在的省/自治区/直辖市。
   - 国家/地区**ISO**代码—贵组织所在的两位数ISO (国际标准化组织)代码、例如美国。
4. 单击 * 下载 * 。

   此时将向本地系统保存一个.csr文件。
5. 将.csr文件发送到CA。

完成后

从密钥管理服务器获取客户端和服务器证书后、请导入这些证书以使用存储阵列控制器进行身份验证。

导入密钥管理服务器证书

对于外部密钥管理、您可以在存储阵列和密钥管理服务器之间导入用于身份验证的证书、以便这两个实体可以相互信任。证书有两种类型：客户端证书用于验证控制器、而密钥管理服务器证书用于验证服务器。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 存储阵列具有可用的客户端证书。

  客户端证书用于验证存储阵列的控制器、以便密钥管理服务器可以信任其IP地址。要获取客户端证书、您必须完成存储阵列的CSR、然后将其上传到密钥管理服务器。从服务器生成客户端证书。
- 密钥管理服务器证书可用。

  密钥管理服务器证书用于验证服务器、以便存储阵列可以信任其IP地址。要获取密钥管理服务器证书、必须从密钥管理服务器生成该证书。

关于此任务

此任务介绍如何在存储阵列控制器和密钥管理服务器之间上传用于身份验证的证书文件。

步骤

1. 选择菜单：设置[证书]。
2. 从*密钥管理*选项卡中、选择*导入*。

此时将打开一个对话框、用于导入证书文件。

3. 单击*浏览*按钮以选择文件。

   文件名显示在对话框中。

4. 单击 * 导入 * 。

   文件已上传并进行验证。

导出密钥管理服务器证书

您可以将密钥管理服务器的证书保存到本地计算机。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 必须事先导入证书。

步骤

1. 选择菜单：设置[证书]。
2. 选择*密钥管理*选项卡。
3. 从表中、选择要导出的证书、然后单击*导出*。

   此时将打开保存对话框。

4. 输入文件名并单击*保存*。

启用证书撤消检查

您可以启用对已撤销证书的自动检查、以便联机证书状态协议(OCSP)服务器阻止用户进行非安全连接。如果证书颁发机构(CA)颁发的证书不正确或私钥受到损坏、则自动撤消检查非常有用。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 在两个控制器上都配置了DNS服务器、这样可以为OCSP服务器使用完全限定域名。此任务可从硬件页面访问。
- 如果要指定自己的OCSP服务器、则必须知道该服务器的URL。

关于此任务

在此任务期间、您可以配置OCSP服务器或使用证书文件中指定的服务器。OCSP服务器会确定CA是否已在计划的到期日期之前撤销任何证书、然后在证书被撤销时阻止用户访问站点。

步骤

1. 选择菜单：设置[证书]。
2. 选择*可信*选项卡。

您还可以从密钥管理选项卡启用撤消检查。

3. 单击*不常见任务*、然后从下拉菜单中选择*启用撤消检查*。
4. 选择*我要启用撤消检查*、以便复选框中显示复选标记、对话框中显示其他字段。
5. 在* OCSP响应器地址*字段中、您可以选择输入OCSP响应器服务器的URL。如果不输入地址、系统将使用证书文件中的OCSP服务器URL。
6. 单击*测试地址*以确保系统可以打开与指定URL的连接。
7. 单击 * 保存 * 。

结果

如果存储阵列尝试使用已撤销的证书连接到服务器、则连接将被拒绝并记录事件。

常见问题解答

为什么会显示"无法访问其他控制器"对话框?

在执行与CA证书相关的某些操作(例如、导入证书)时、您可能会看到一个对话框、提示您接受第二个控制器的自签名证书。

在具有两个控制器的存储阵列(双工配置)中、如果SANtricity 系统管理器无法与第二个控制器通信、或者您的浏览器在操作的某个时间点无法接受证书、则有时会显示此对话框。

如果此对话框打开、请单击*接受自签名证书*以继续。如果另一个对话框提示您输入密码、请输入用于访问System Manager的管理员密码。

如果此对话框再次出现、并且您无法完成证书任务、请尝试以下过程之一：

- 使用其他浏览器类型访问此控制器、接受证书并继续。
- 使用System Manager访问第二个控制器、接受自签名证书、然后返回到第一个控制器并继续。

如何知道需要将哪些证书上传到**System Manager**?

对于外部密钥管理、您可以导入两种类型的证书、以便在存储阵列和密钥管理服务器之间进行身份验证、从而使这两个实体可以相互信任。

客户端证书用于验证存储阵列的控制器、以便密钥管理服务器可以信任其IP地址。要获取客户端证书、您必须完成存储阵列的CSR、然后将其上传到密钥管理服务器。从服务器生成客户端证书、然后使用System Manager导入该证书。

密钥管理服务器证书用于验证密钥管理服务器、以便存储阵列可以信任其IP地址。要获取密钥管理服务器证书、必须从密钥管理服务器生成该证书。

关于证书撤消检查、我需要了解哪些信息?

使用System Manager、您可以使用联机证书状态协议(Online Certificate Status Protocol、OCSP)服务器来检查已撤销的证书、而不是上传证书撤消列表(Certificate Revocation

List、CRL)。

已撤销的证书不应再受信任。证书可能会因多种原因而被撤销；例如、如果证书颁发机构(CA)颁发的证书不正确、私钥被泄露或标识的实体不符合策略要求。

在System Manager中与OCSP服务器建立连接后、存储阵列将在连接到AutoSupport 服务器、外部密钥管理服务器(External Key Management Server、EKMS)、基于SSL的轻型目录访问协议(Lightweight Directory Access Protocol over SSL、LDAPS)服务器或系统日志服务器时执行撤消检查。存储阵列会尝试验证这些服务器的证书、以确保它们未被撤消。然后、服务器将为该证书返回"good "、"revoked"或"unknown"值。如果证书已撤销或阵列无法与OCSP服务器联系、则连接将被拒绝。

在System Manager或命令行界面(CLI)中指定OCSP响应程序地址会覆盖在证书文件中找到的OCSP地址。

将为哪些类型的服务器启用撤消检查?

每当存储阵列连接到AutoSupport 服务器、外部密钥管理服务器(External Key Management Server、EKMS)、基于SSL的轻型目录访问协议(Lightweight Directory Access Protocol over SSL、LDAPS)服务器或系统日志服务器时、它都会执行撤消检查。